REMARKS

In response to the Office Action mailed October 27, 2009, Applicants respectfully request reconsideration. To further the prosecution of this Application, Applicants submit the following remarks and have added a new claim. The claims as now presented are believed to be in allowable condition.

Claims 1-15, 21-25, 31, 33, 35, and 37 were pending in this Application (with claims 32, 34, 36, and 38 withdrawn from consideration). By this Amendment, claim 39 has been added. Accordingly, claims 1-15, 21-25, 31, 33, 35, 37, and 39 are now pending in this Application. Claims 1, 6, 11, and 21 are independent claims.

Rejections under § 103

Claims 1-15 and 21-25 were rejected under 35 U.S.C. § 103(a) as being unpatentable over "Network Intrusion Detection: Evasion, Traffic Normalization, and End-to-End Protocol Semantics," by Mark Handley and Vern Paxson (hereinafter Handley) in view of U.S. Patent No. 6,192,404 (Hurst, et al.). Claims 31, 33, 35, and 37 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Handley in view of Hurst, and further in view of U.S. Patent Publication No. 2003/0009594 (McElligott).

Applicants respectfully traverse these rejections and request reconsideration. The claims are in allowable condition.

Handley teaches several methods by which an attacker can evade detection by a network intrusion detection system (NIDS) by exploiting ambiguities (Pages 1-3). In particular, one ambiguity that is discussed includes the situation in which a packet arrives at a NIDS with a value in its time-to-live (TTL) field which is too small to allow it to reach its destination end-system. This is noted to be problematic because the NIDS may then have an incorrect model of the protocol state of the end-system, allowing an attacker to covertly issue

malicious commands (Page 2, Col. 1, item iii and Figure 1). Handley then discloses a normalizer which is capable of altering packets to remove certain ambiguities to prevent these kinds of attacks from succeeding (Pages 3-15). In one situation, the Handley normalizer attempts to prevent an attacker from finding a way to systematically ensure that some packets will be received by an end-system of the NIDS and some not. In particular, if a packet arrives at the NIDS with a value in its time-to-live (TTL) field which is too small to allow it to reach the end-system, the Handley normalizer increases the original value in the TTL field to a larger value so that the packet reaches the end-system. Handley calls this larger value the "minimum" since it is just large enough to ensure that the packet does reach the end-system (Page 4, Col. 2, fourth paragraph and Page 9, Col. 1, at TTL solution #3).

Hurst teaches a technique for determining the TTL distance to other nodes of a computer network very quickly (Abstract). This is done so that multicast messages can be sent to a portion of a network by setting the TTL parameter of that message to be equal to the TTL distance of the target computer furthest from the source (Col. 1, line 45 through Col. 2, line 35). This is done by having a source computer 102A send a set of multicast TTL query messages, each member of the set having a different initial TTL parameter (in the header) and each member of the set also storing the corresponding value of the initial TTL parameter in the body of that message (Col. 5, line 50 through Col. 6, line 18). Recipient computer 102R, upon receiving each TTL query message, processes that message by comparing the TTL parameter of the received packet to a minimum TTL parameter value 314 stored in TTL determining logic 310 of recipient computer 102R and updating the value of the minimum TTL parameter value 314 stored in the TTL determining logic 310 if the TTL parameter of the received packet is less than the value of the minimum TTL parameter value 314 stored in the TTL determining logic 310 (Col. 7, lines 15-32). This allows each receiving node to determine its TTL distance from source computer 102A by

reference to the final value of the minimum TTL parameter value 314 stored in the TTL determining logic 310 of that node (Col. 3, lines 24-29).

McElligott is directed to techniques for identifying the geographical location of a device (Abstract).

Claims 1-5 and 31

Claim 1 recites a method 400 (see Fig. 4) of blocking attacks on a protected computer network 240 (see Fig. 2). The method includes (a) receiving a plurality of packets 250 (see Fig. 2) from a network 220 (see Fig. 2), each packet 250 having a packet time to live (TTL) value 254 (see Fig. 2 and Par. [0017]) and belonging to a corresponding packet flow (see Par. [0024] and step 410 of Fig. 4), (b) storing the smallest packet TTL value 254 (see TTL store 324 of Fig. 3) received from each corresponding packet flow (see Par. [0025] and steps 420, 430, 440 of Fig. 4), and (c) prior to transmitting (step 460 of Fig. 4) each packet 250, setting the packet TTL value 254B (see Fig. 2) to the smallest packet TTL value received (see TTL store 324 of Fig. 3) for the corresponding packet flow (see Par. [0026] and step 450 of Fig. 4).

The cited reference does not teach a method which includes, prior to transmitting each packet, *setting a packet TTL value to the smallest packet TTL value received for a corresponding packet flow*. In contrast, Handley discloses a normalizer which **raises** the TTL of an incoming packet to a **minimum-acceptable value** in order to ensure that the packet will be able to reach any point within the internal network without timing out (Page 4, Col. 2, fourth paragraph and Page 9, Col. 1, at TTL solution #3), while Hurst is directed to techniques for determining the TTL distance to other nodes of a computer network very quickly (Abstract).

First, a person having ordinary skill in the art (PHOSITA) would not think to combine Hurst with Handley because **these two references operate**

according to entirely different principles. Handley is about raising a packet TTL of an incoming packet in order to ensure that the packet will be able to reach any point within the internal network without timing out, thereby **protecting against attack**. On the other hand, **Hurst is about determining the TTL distance to other computers in a network**. No PHOSITA would think to combine these disparate techniques. Indeed, there would be no likelihood of success. The Office Action, on page 3, asserts that Hurst is needed to teach lowering a TTL value rather than raising a TTL value as in Handley[1], but the essence of the technique for protecting the network in Handley relies on the fact that the TTL value of an incoming packet is raised. **Merely incorporating the concept of lowering a TTL value from a reference that is completely unrelated to protecting against network attacks would be ludicrous because a PHOSITA would have no reason to believe that there would be any benefit in radically altering the network protection technique of Handley**. Even if Hurst teaches the idea of lowering a TTL value (and Applicants do not admit this, see below), it does not make any sense to just export that idea into an unrelated technique that operates according to different principles. Furthermore, **it is clear that claim 1 and the technique of Handley operate according to entirely different principles (see section VII.1.c of the Appeal Brief** filed on July 24, 2009, all of whose arguments have been deemed persuasive), and that lends further support to the argument that merely adding a reference to teach a narrow technical concept is insufficient to render the combination obvious.

Second, neither Handley nor Hurst actually teaches *setting a packet TTL value to the smallest packet TTL value received for a corresponding packet flow*. The Office Action, on page 3, cites Col. 7, lines 27-31 of Hurst as teaching this feature. However, in fact, **that portion of Hurst teaches no such thing**! Rather,

[1] Although, applicants intend to also argue that the Office Action has mischaracterized Hurst in this regard. See below.

that portion is about updating a minimum TTL parameter value 314 stored in determining logic 310 of a recipient computer 102R based on a TTL parameter value of a received packet. Although minimum TTL parameter value 314 can indeed be decreased, minimum TTL parameter value 314 is not a ***packet*** *TTL value* because it is not part of a packet at all, but is rather a variable that stores information about what the minimum value of all the TTL parameters of all the TTL query packets received is. Even if Hurst teaches how to calculate the minimum TTL parameter received, that value is not actually ever used to *set* a *packet TTL value*. This point is further clarified by newly added dependent claim 39.

For the reasons stated above, claim 1 patentably distinguishes over the cited prior art, and the rejection of claim 1 under 35 U.S.C. §103(a) should be withdrawn. Accordingly, claim 1 is in allowable condition.

Because claims 2-5 and 31 depend from and further limit claim 1, claims 2-5 and 31 are in allowable condition for at least the same reasons. Additionally, it should be understood that the dependent claims recite additional features which further patentably distinguish over the cited prior art.

For example, **claim 31** recites the method of Claim 1, wherein storing (see steps 430 and 440 of Fig. 4) the smallest packet TTL 254A (see Fig. 2) value received from each said corresponding packet flow includes, for each said packet, (a) if that packet 250 (see Fig. 2) is the first packet received from said corresponding packet flow, then storing the packet TTL value 254A of that packet 250 as said smallest packet TTL value received from said corresponding packet flow (Pars. [0019]-[0025]), (b) if that packet 250 is not the first packet received from said corresponding packet flow and the packet TTL value of that packet is less than (see step 430 of Fig. 4) the stored smallest packet TTL value received from said corresponding packet flow (see Par. 0025]), then storing (see step 440 of Fig. 4) the packet TTL value 254A of that packet 250 as said smallest packet TTL value received from said corresponding packet flow (see Par. 0025]), and (c)

if that packet 250 is not the first packet received from said corresponding packet flow and the packet TTL value 254A of that packet is greater than the stored smallest packet TTL value received from said corresponding packet flow, then refraining (see step 435 of Fig. 4) from storing the packet TTL value 254A of that packet 250 as said smallest packet TTL value received from said corresponding packet flow.

The Office Action, on pages 5-7, rejected claim 31 on the basis of a combination of Handley, Hurst, and McElligott. However, it is clear that Hurst is only mentioned because it was needed for the rejection of parent claim 1. Thus, the rejection of the substance of claim 31 is **exactly word-for-word** (except for added passing mentions of the Hurst reference) the same as the rejection of claim 31 presented in the last Office Action (dated December 8, 2008). As previously argued in section VII.2 of the **Appeal Brief** filed on July 24, 2009 (all of whose arguments have been deemed persuasive), Handley is directed towards techniques for preventing attacks on a network through the use of a normalizer. McElligott, on the other hand, is directed to techniques for identifying the geographical location of a device (Abstract). These fields are unrelated, and it is unclear why any person having ordinary skill in the art would be motivated to combine these references. The Office Action, on page 7, presents an argument as to why a person having ordinary skill in the art would have combined Handley with McElligot, however, that argument does not actually explain why a person having ordinary skill in the art would be motivated to combine the references. Rather, it merely explains that McElligot teaches **how** to determine if a TTL is lower than a stored value. However, because preventing attacks on a network is completely unrelated to identifying the geographical location of a device, there is no motivation to combine these references. Moreover, no other explanation as to why it would be obvious has been provided. Thus, it would not have been obvious to a person having ordinary skill in the art at the time of the invention to have combined Handley with McElligot.

Indeed, this argument was made previously in the Appeal Brief, and the Office Action, on page 2, has noted that "**Applicant's arguments within** the last correspondence [i.e., **the Appeal Brief] have been deemed persuasive**." Thus, the continued rejection of claim 31 under the same basis as in the previous Office Action is unwarranted and therefore **the rejection of claim 31 is defective on its face**. See MPEP § 707.07(f). Indeed, no response has been given to Applicants' argument that it would not have been obvious to combine Handley with McElligott, and therefore Applicants are unable to respond to the Office Action's continued rejection of claim 31 except by repeating the same arguments that were presented before (which were deemed persuasive). Therefore, **the rejection of claim 31 must be withdrawn**.

Claims 6-15, 21-25, 33, 35, and 37

Claims 6, 11, and 21 recite limitations which are similar to the limitations of claim 1. Accordingly, claims 6, 11, and 21 distinguish over the prior art for reasons similar to those presented above in connection with claim 1.

For the reasons stated above, claims 6, 11, and 21 patentably distinguish over the cited prior art, and the rejection of claims 6, 11, and 21 under 35 U.S.C. §103(a) should be withdrawn. Accordingly, claims 6, 11, and 21 are in allowable condition.

Because claims 7-10 and 33 depend from and further limit claim 6, claims 7-10 and 33 are in allowable condition for at least the same reasons. Additionally, it should be understood that the dependent claims recite additional features which further patentably distinguish over the cited prior art.

Because claims 12-15 and 35 depend from and further limit claim 11, claims 12-15 and 35 are in allowable condition for at least the same reasons. Additionally, it should be understood that the dependent claims recite additional features which further patentably distinguish over the cited prior art.

Because claims 22-25 and 37 depend from and further limit claim 21, claims 22-25 and 37 are in allowable condition for at least the same reasons. Additionally, it should be understood that the dependent claims recite additional features which further patentably distinguish over the cited prior art.

Newly Added Claims

Claim 39 has been added and is believed to be in allowable condition. Claim 39 depends from claim 1. Support for claim 39 is provided within the Specification, for example, in Figs. 1-2 and Pars. [0016]-[0021]. No new matter has been added.

Conclusion

In view of the foregoing remarks, this Application should be in condition for allowance. A Notice to this effect is respectfully requested. If the Examiner believes, after this Amendment, that the Application is not in condition for allowance, the Examiner is respectfully requested to call the Applicants' Representative at the number below.

Applicants hereby petition for any extension of time which is required to maintain the pendency of this case. If there is a fee occasioned by this Amendment, including an extension fee, please charge any deficiency to Deposit Account No. 50-3661.

If the enclosed papers or fees are considered incomplete, the Patent Office is respectfully requested to contact the undersigned collect at (508) 616-2900, in Westborough, Massachusetts.

Respectfully submitted,

/Michael Ari Behar/

M. Ari Behar, Esq.
Attorney for Applicants
Registration No.: 58,203
Bainwood, Huang & Associates, L.L.C.
Highpoint Center
2 Connector Road
Westborough, Massachusetts 01581
Telephone: (508) 616-2900
Facsimile: (508) 366-4688

Attorney Docket No.: 1004-128

Dated: January 27, 2010